



UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
09/784,512	02/14/2001	David C. Platt	TIVO0067	3300

29989 7590 09/20/2004

HICKMAN PALERMO TRUONG & BECKER, LLP
1600 WILLOW STREET
SAN JOSE, CA 95125

EXAMINER

CHAI, LONGBIT

ART UNIT PAPER NUMBER

2131

DATE MAILED: 09/20/2004

5

Please find below and/or attached an Office communication concerning this application or proceeding.

Office Action Summary

Application No.

09/784,512

Applicant(s)

PLATT, DAVID

Examiner

Longbit Chai

Art Unit

2131

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --

Period for Reply

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE 3 MONTH(S) FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If the period for reply specified above is less than thirty (30) days, a reply within the statutory minimum of thirty (30) days will be considered timely.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133). Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

Status

- 1) ☒ Responsive to communication(s) filed on 14 April 2004.
- 2a) ☐ This action is **FINAL**. 2b) ☒ This action is non-final.
- 3) ☐ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

Disposition of Claims

- 4) ☐ Claim(s) _____ is/are pending in the application.
- 4a) Of the above claim(s) _____ is/are withdrawn from consideration.
- 5) ☐ Claim(s) _____ is/are allowed.
- 6) ☒ Claim(s) 1-26 is/are rejected.
- 7) ☐ Claim(s) _____ is/are objected to.
- 8) ☐ Claim(s) _____ are subject to restriction and/or election requirement.

Application Papers

- 9) ☐ The specification is objected to by the Examiner.
- 10) ☒ The drawing(s) filed on 14 February 2001 is/are: a) ☒ accepted or b) ☐ objected to by the Examiner.
Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).
Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).
- 11) ☐ The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

Priority under 35 U.S.C. § 119

- 12) ☐ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).
- a) ☐ All b) ☐ Some * c) ☐ None of:
1. ☐ Certified copies of the priority documents have been received.
2. ☐ Certified copies of the priority documents have been received in Application No. _____.
3. ☐ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).
- * See the attached detailed Office action for a list of the certified copies not received.

Attachment(s)

- 1) ☒ Notice of References Cited (PTO-892)
- 2) ☐ Notice of Draftsperson's Patent Drawing Review (PTO-948)
- 3) ☐ Information Disclosure Statement(s) (PTO-1449 or PTO/SB/08)
Paper No(s)/Mail Date _____.
- 4) ☐ Interview Summary (PTO-413)
Paper No(s)/Mail Date. _____.
- 5) ☐ Notice of Informal Patent Application (PTO-152)
- 6) ☐ Other: _____.

DETAILED ACTION

Priority

1. No claim for priority has been made in this application.

The effective filing date for the subject matter defined in the pending claims in this application is 2/14/2001.

Claim Rejections - 35 USC § 102

(e) the invention was described in (1) an application for patent, published under section 122(b), by another filed in the United States before the invention by the applicant for patent or (2) a patent granted on an application for patent by another filed in the United States before the invention by the applicant for patent, except that an international application filed under the treaty defined in section 351(a) shall have the effects for purposes of this subsection of an application filed in the United States only if the international application designated the United States and was published under Article 21(2) of such treaty in the English language.

2. Claim 25 is rejected under 35 U.S.C. 102(e) as being anticipated by Daniel (Patent Number: US 6766301 B1), hereinafter referred to as Daniel.
3. As per claim 25, Daniel teaches a method for preventing security leak of authentication number database, comprising the steps of:
 - a. keeping said authentication number database behind a firewall (Daniel: see for example, Column 4 Line 62 – 66, Column 8 Line 45 – 47 and Figure 1 Element 7); and
 - b. denying access of unauthorized machines (Daniel: see for example, Figure 6 Element 88).

4. Claim 10 is rejected under 35 U.S.C. 102(e) as being anticipated by Mankoff (Patent Number: US 6385591 B1), hereinafter referred to as Mankoff.

5. As per claim 10, Mankoff teaches a method for generating a coupon authentication number for each receiving device coupled to a coupon distribution system, comprising the steps of:

- a. activating said receiving device (Mankoff: see for example, Column 5 Line 26 – 46);
- b. generating a coupon authentication number for each said receiving device, wherein said coupon authentication number is randomly given and can be of any length of bits long (Mankoff: see for example, Column 5 Line 31);
- c. storing said coupon authentication number in said coupon authentication number database (Mankoff: see for example, Figure 1 Element 27, Column 3 Line 50 – 54 and Column 2 Line 15 – 17);
- d. communicating said coupon authentication number to said key server (Mankoff: see for example, Column 5 Line 46);
- e. encrypting said coupon authentication number (Mankoff: see for example, Column 5 Line 35 – 37); and
- f. sending encrypted coupon authentication number to said receiving device which adds said encrypted coupon authentication number to said receiving device's keyring as a coupon key (Mankoff: see for example, Column 5 Line 35 – 37).

Claim Rejections - 35 USC § 103

The following is a quotation of 35 U.S.C. 103(a) which forms the basis for all obviousness rejections set forth in this Office action:

(a) A patent may not be obtained though the invention is not identically disclosed or described as set forth in section 102 of this title, if the differences between the subject matter sought to be patented and the prior art are such that the subject matter as a whole would have been obvious at the time the invention was made to a person having ordinary skill in the art to which said subject matter pertains. Patentability shall not be negated by the manner in which the invention was made.

6. Claims 1 – 4, 11 and 12 are rejected under 35 U.S.C. 103(a) as being unpatentable over Mankoff (Patent Number: US 6385591 B1), hereinafter referred to as Mankoff, in view of Gressel (Patent Number: 5852665), hereinafter referred to as Gressel.

7. As per claim 1, Mankoff teaches a process for generating, delivery, and validation of electronic coupons via a telecommunication system, comprising the sub-processes of:

- a. generating a coupon authentication number for each receiving device (Mankoff: see for example, Column 5 Line 26 – 46);
- b. delivering a cryptographic electronic coupon to one or more receiving devices (Mankoff: see for example, Column 5 Line 26 – 46);
- c. validating said cryptographic coupon when a user applies to redeem said cryptographic coupon (Mankoff: see for example, Column 5 Line 43 – 46);
- d. wherein said telecommunication system includes a service center, a plurality of receiving devices, a display device coupled to each receiving device, a communication

channel connecting said service center and each receiving device (Mankoff: see for example, Figure 1);

e. wherein said service center comprises an activation database, an authentication number database and a key server (Mankoff: see for example, Figure 1, Column 3 Line 50 – 54 and Column 2 Line 15 – 17);

8. Mankoff does not disclose expressly said receiving device comprises a persistent storage device which stores one or more public keys assigned to said receiving device, and a crypto-chip which stores one or more private keys assigned to said receiving device.

9. Gressel teaches:

f. wherein said receiving device comprises a persistent storage device which stores one or more public keys assigned to said receiving device, and a crypto-chip which stores one or more private keys assigned to said receiving device (Gressel: see for example, Column 5 Line 26 and Column 9 Line 8).

10. It would have been obvious to a person of ordinary skill in the art at the time the invention was made to combine the teaching of Gressel within the system of Mankoff because (a) Mankoff discloses the secured communications to the receiving device can use SSL (Secured Socket Layer) (Mankoff: see for example, Column 52 Line 35 – 37) and (b) Gressel teaches the encrypting methods of the session key for SSL (Gressel: see for example, Column 5 Line 23 – 27).

g. wherein said communication channel may be a telephone modem, a cable modem, or a local area network (Mankoff: see for example, Figure 1).

11. As per claim 2, Mankoff as modified teaches the claimed invention as described above (see claim 1). Mankoff as modified further teaches the process comprises the steps of:

- a. activating said receiving device (Mankoff: see for example, Column 5 Line 26 – 46);
- b. generating a coupon authentication number for each said receiving device, wherein said coupon authentication number is randomly given and can be of any length of bits long (Mankoff: see for example, Column 5 Line 31);
- c. storing said coupon authentication number in said coupon authentication number database (Mankoff: see for example, Figure 1 Element 27, Column 3 Line 50 – 54 and Column 2 Line 15 – 17);
- d. communicating said coupon authentication number to said key server (Mankoff: see for example, Column 5 Line 46);
- e. encrypting said coupon authentication number (Mankoff: see for example, Column 5 Line 35 – 37); and
- f. sending encrypted coupon authentication number to said receiving device which adds said encrypted coupon authentication number to said receiving device's keyring as a coupon key (Mankoff: see for example, Column 5 Line 35 – 37).

12. As per claim 3 and 11, Mankoff as modified teaches the claimed invention as described above (see claim 2 and 10 respectively). Mankoff as modified further teaches step of encrypting said coupon authentication number is performed by said key server

Art Unit: 2131

using said receiving device's El Gamal public key which is stored both in said activation database and said receiving device's persistent storing device (Mankoff: see for example, Column 5 Line 36: Mankoff teaches using appropriate encryption scheme for the verification code (e.g. PGP) – “El Gamal algorithm” is one of the commonly used ciphering algorithms by PGP).

13. As per claim 4 and 12, Mankoff as modified teaches the claimed invention as described above (see claim 2 and 10 respectively). Mankoff as modified further teaches embedding a date or time stamp in said coupon key for convenience to replace said authentication number when ever said authentication number database is compromised (Mankoff: see for example, Column 5 Line 33: Mankoff teaches the coupon also includes Expiration Date (which has a date or time stamp) besides the unique coupon number and thereby it is possible to replace said authentication number when ever said authentication number database is compromised).

14. Claims 5 – 9 and 13 – 24 are rejected under 35 U.S.C. 103(a) as being unpatentable over Mankoff (Patent Number: US 6385591 B1), hereinafter referred to as Mankoff, in view of Freeman (Patent Number: US 6450407 B1), hereinafter referred to as Freeman, and in view of Gressel (Patent Number: 5852665), hereinafter referred to as Gressel.

15. As per claim 18, Mankoff teaches a system for coupon encryption, distribution, and validation, comprising:

Art Unit: 2131

a. an information service center which comprises an activation database, a coupon authentication number database, and a key server (Mankoff: see for example, Column 5 Line 26 – 46);

16. Mankoff does not disclose expressly a client which issues coupons, each of said coupons is designated a unique offer ID number.

17. Freeman teaches:

b. a client which issues coupons, each of said coupons is designated a unique offer ID number (Freeman: see for example, Column 3 Line 2 – 4: The coupon U.P.C. which includes Manufacturer ID Code and Product Family Code is qualified as a Coupon Offer ID number);

18. It would have been obvious to a person of ordinary skill in the art at the time the invention was made to combine the teaching of Freeman within the system of Mankoff because (a) Mankoff discloses the coupon validity checks at the server can be based on a verification code such as checksum (or the like) – i.e., the hash result (Mankoff: see for example, Column 5 Line 26 – 46) and (b) Freeman teaches the validation of a coupon should base on the offer number (i.e. representing a specific product) (Freeman: see for example, Column 3 Line 2 – 4. Therefore, the context applied to the hash function is indeed the coupon offer number.

19. Mankoff as modified further teaches:

c. a plurality of service receiving devices, each of which is coupled to a displaying device (Freeman: see for example, Column 15 Line 54 – 59);

Art Unit: 2131

- d. a channel through which said information service center and said service receiving device communicate (Mankoff: see for example, Column 5 Line 26 – 46);
 - e. wherein said information service center generates a coupon authentication number for each said service receiving device, wherein said coupon authentication number is stored in said coupon authentication number database and is communicated to said key server (Mankoff: see for example, Column 5 Line 26 – 46);
 - f. wherein said key server encrypts said coupon authentication number using El Gamal algorithm and sends encrypted authentication number to said service receiving device (Mankoff: see for example, Column 5 Line 36: Mankoff teaches using appropriate encryption scheme for the verification code (e.g. PGP) – “El Gamal algorithm” is one of the commonly used ciphering algorithms by PGP);
20. Mankoff teaches service receiving device comprises a hard drive (Mankoff: see for example, Figure 1 Element 12).
21. Mankoff does not teach service receiving device comprises a crypto-chip.
22. Gressel teaches:
- g. wherein said service receiving device comprises a crypto-chip (Gressel: see for example, Column 9 Line 8);
23. It would have been obvious to a person of ordinary skill in the art at the time the invention was made to combine the teaching of Gressel within the system of Mankoff because Gressel discloses a fast hardware ciphering technique to enhance the system performance.

Art Unit: 2131

24. Mankoff teaches the receiving device should obtain a verifying code (or hash result) (Mankoff: see for example, Column 5 Line 31 – 32) associated with a hash function and the hash context is the coupon serial number (see above).

25. Mankoff does not teach expressly performing the hash function locally at the user receiving device by receiving the hash key (i.e. coupon authentication number) from the server.

26. However, it would have been obvious to a person of ordinary skill in the art at the time the invention was made to modify obtaining the hash result remotely (i.e. at the server side and then passing to the user) to accommodate performing the hash result locally at the user side (by receiving the hash key and context from the remote server) because, for the receiving device, both ways serve the same purpose to obtain the hash result so that, subsequently, this returned hash result sent by the user can be validated at the server. Besides, both approaches also effectively use encryption to protect the sensitive data during the transmissions.

h. wherein said crypto-chip performs a hash operation on said offer ID number using said encrypted coupon authentication number and takes the first or last N digits of the hashed result as a coupon ID number for said coupon (Gressel: see for example, Column 9 Line 8: For crypto-chip, both ciphering and hashing functions can be performed on a cryptoprocessor) & (Mankoff: see for example, Column 5 Line 32: Checksum is one kind of N digits of the hash results); and

i. wherein said coupon may be validated by said key server, which uses said service receiving device's serial number to look up the unencrypted coupon

Art Unit: 2131

authentication number stored in said coupon authentication number database (Mankoff: see for example, Column 5 Line 43 – 46).

27. and performs a hash operation on said offer ID number using said unencrypted coupon authentication number and compares a base number taken from the first or last N digits of the hashed result with said coupon ID number submitted, and validates said coupon if said base number and said coupon number match (see same rationale addressed above).

28. As per claim 13, claim 13 does not further teach over claim 18. Therefore, see rationale addressed above in rejecting claim 18.

29. As per claim 17, claim 17 encompasses the scope at least as described in claim 18 and besides that, in further regards to claim 17, Mainkoff as modified further teaches receiving device's serial number, and said coupon ID number by said vendor who accesses to a common gateway interface (CGI) at said service center (Mankoff: see for example, Column 3 Line 8).

30. As per claim 9, Mankoff as modified teaches the claimed invention as described above (see claim 1). Mankoff as modified does not further teach over the claim 17.

31. As per claim 5, Mankoff as modified teaches the claimed invention as described above (see claim 1). Mankoff as modified does not further teach over the claim 13.

32. As per claim 6 and 14, Mankoff as modified teaches the claimed invention as described above (see claim 5 and 13 respectively). Mankoff as modified further teaches confirming a unique offer ID number for said coupon comprises the sub-steps of:

a. checking whether or not said client has designated a unique offer ID number for said coupon (Freeman: see for example, Column 3 Line 2 – 4: The coupon U.P.C. which includes Manufacturer ID Code and Product Family Code is qualified as a Coupon Offer ID number);

b. wherein if said client has designated a unique offer ID number for said coupon, checking the uniqueness of said offer ID number and resolving possible collisions with other offers (Freeman: see for example, Column 3 Line 2 – 4); and

c. wherein if said client has not designated a unique offer ID number for said coupon, generating a unique offer ID number for said coupon (This is evidently one of the design choice if this particular coupon is not rejected or cancelled).

33. As per claims 7, 15 and 23, Mankoff as modified teaches the claimed invention as described above (see claims 5, 13 and 18 respectively). Mankoff as modified further teaches offer ID number is implemented as ASCII character strings (The format of a number is always transformable between different types).

34. As per claims 8, 16 and 24, Mankoff as modified teaches the claimed invention as described above (see claims 6, 13 and 18 respectively). Mankoff as modified further teaches N is 6 (Six as the number of characters is one of the design choices commonly used for an identification code that can also provide proper security).

35. As per claim 9, Mankoff as modified teaches the claimed invention as described above (see claim 1). Mankoff as modified does not further teach over the claim 17.

36. As per claim 19, Mankoff as modified teaches the claimed invention as described above (see claim 18). Mankoff as modified further teaches receiving device is a

Art Unit: 2131

personal video recorder and said displaying device is a TV set (Gressel: see for example, Column 10 Line 30 – 32: Gressel teaches the secured receiving device can be adapted for use with any type of communication devices including TV).

37. As per claim 20, Mankoff as modified teaches the claimed invention as described above (see claim 18). Mankoff as modified further teaches channel is a telephone modem, or a cable modem, or a local area network (Mankoff: see for example, Figure 1).

38. As per claim 21, Mankoff as modified teaches the claimed invention as described above (see claim 18). Mankoff as modified further teaches coupon authentication number is randomly given and can be of any length of bits (random number is widely used in the field to enhance the security).

39. As per claim 22, Mankoff as modified teaches the claimed invention as described above (see claim 18). Mankoff as modified further teaches offer ID number is randomly given and can be of any length of bits (random number is widely used in the field to enhance the security).

40. Claim 26 is rejected under 35 U.S.C. 103(a) as being unpatentable over Daniel (Patent Number: US 6766301 B1), hereinafter referred to as Daniel.

41. As per claim 26, Daniel teaches a method for remedying security leak of authentication number database, comprising the steps of: fixing said security leak (Daniel: see for example, Column 12 Line 13 – 22 and Figure 4 Element 64: Tracing

Art Unit: 2131

and reducing the fraud after any couple anomalies as taught by Daniel is one type of fixing said security leak);

42. Daniel does not disclose expressly generating a new random coupon authentication number for each said receiving device; and distributing said coupon authentication number to said receiving device via said key server.

43. However, it would have been obvious to a person of ordinary skill in the art at the time the invention was made to modify reducing the coupon security fraud to accommodate generating a new random coupon authentication number because Daniels discloses, upon the detection of security fraud from submitted coupons, using the auditing trail which must be evidently accomplished by first deleting the anomaly coupon and then re-generating / re-distributing the new coupon numbers in order to continue to trace / audit the coupon transactions as taught by Daniel (Daniel: see for example, Column 12 Line 13 – 22 and Figure 4 Element 64).


Any inquiry concerning this communication or earlier communications from the examiner should be directed to Longbit Chai whose telephone number is 703-305-0710. The examiner can normally be reached on Monday-Friday 8:00am-5:00pm.

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Ayaz R Sheikh can be reached on 703-305-9648. The fax phone number for the organization where this application or proceeding is assigned is 703-872-9306.

Information regarding the status of an application may be obtained from the Patent Application Information Retrieval (PAIR) system. Status information for published applications may be obtained from either Private PAIR or Public PAIR. Status information for unpublished applications is available through Private PAIR only. For more information about the PAIR system, see <http://pair-direct.uspto.gov>. Should you have questions on access to the Private PAIR system, contact the Electronic Business Center (EBC) at 866-217-9197 (toll-free).

Longbit Chai
Examiner
Art Unit 2131

LBC


AYAZ SHEIKH
SUPERVISORY PATENT EXAMINER
TECHNOLOGY CENTER 2100